FortiOS - Release Notes

Version 6.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 31, 2020
FortiOS 6.4.0 Release Notes
01-640-596064-20200331

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-03-31	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.4.0 build 1579.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.0 supports the following models.

FortiGate	FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-100E, FG-100EF, FG-101E, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.4.0 images are delivered on request and are not available on the Beta portal.

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

Application group improvements

Bug ID	Description
565309	*Application Group* improvements.

NGFW mode

Bug ID	Description
584314	NGFW mode should have a link to show list of all applications.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

CLI and GUI behavior changes

Bug ID	Description
610191	This change includes multiple behaviour changes to both the CLI and GUI: • Added default automation rules (after factory reset). All are disabled by default, except for the FEXP push notification. • Added new incoming webhook trigger for automation. • Removed *Email Alert Settings* page. • Added new API for `POST /api/v2/monitor/system/automation-stitch/webhook/<trigger mkey>`.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. Please see the Resolved issues on page 36 section. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

Managed switch controller in NAC policy

Bug ID	Description
621785	`user.nac-policy[].switch-scope` may contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, they need to remove this reference prior to deleting the `managed-switch`.

VLANs on a FortiLink interface

Bug ID	Description
622812	VLANs on a FortiLink interface configured to use a hardware switch may fail to come up after upgrading or rebooting due to an incorrect registration of the IP address of the switch VLAN interface. This issue affects the FG-60E, FG-61E, FG-80E, FG-81E, FG-90E, and FG-91E models that contain a hardware switch and have FortiLink configured on it by default. Aggregate, physical, and software switch interfaces are unaffected.

Bug ID	Description
	Workaround (not reboot persistent): Re-configure the IP address on each VLAN interface to a different IP address. You may use an IP address in the same subnet and then change it back to the original IP address if desired.

Changes in CLI

Bug ID	Description
564318	Move `frequency-handoff/ap-handoff` from radio level to AP level.
571819	Collect EIP from cloud-VMS (Azure, AWS, GCP, AliCloud, and OCI). `pcui-cloudinit-test # execute <?>` **`update-eip Update external IP. <==added`** `config sys interface` `edit [Name]` **`set eip <==added`** `next` `end`
573330	Add `external-web-format` setting under `captive-portal` VAP when external portal is selected. `config wireless-controller vap` `edit guestwifi` `set ssid "GuestWiFi"` `set security captive-portal` `set external-web "http://170.00.00.000/portal/index.php"` `set selected-usergroups "Guest-group"` `set intra-vap-privacy enable` `set schedule "always"` **`set external-web-format auto-detect <==added`** `next` `end`
574588	Add GRE and L2TP support in WiFi. **`config wireless-controller wag-profile <==added`** **`edit [Profile Name] <==added`** `end` `config wireless-controller vap` `edit "80e_gre"` `set ssid "FOS-QA_Bruce_80e_gre"` `set local-bridging enable` `set vlanid 3135` **`set primary-wag-profile "tunnel" <==added`** **`set secondary-wag-profile "l2tp" <==added`** `next` `end`

Bug ID	Description
574882	FAP-U431F and FAP-U433F can support 802.11ax on 2.4 GHz `radio-2` when the platform mode is `single-5G`. `config wireless-controller wtp-profile` `edit "FAPU431F-default"` `config platform` `set type U431F` `set mode single-5G` `end` `config radio-1` `set band 802.11ax-5G` `end` `config radio-2` **`set band 802.11ax`** `end` `config radio-3` `set mode monitor` `end` `next` `end`
586163	Remove `acct-interim-interval` in `vap` configuration.
593968	To populate the interface bandwidth into the interface widget, `set monitor-bandwidth` must be enabled. `config system interface` `edit "port1"` `set vdom "root"` `set ip 10.111.255.86 255.255.255.0` `set allowaccess ping` `set type physical` **`set monitor-bandwidth enable`** `set snmp-index 1` `next` `end`
601345	No warning is shown in GUI when FortiGuard filtering protocol/port setting is not saved.
608185	Resource record limit is now a configurable value for DNS slaves can be edited per `dns-zone`. The `rr-max attribute` for DNS slaves was added. The maximum number of resource records is an integer: 10–65536, or infinite is 0; the default is 16384. `config system dns-database` `edit "slave"` `set domain "fm.tvssa.net"` `set type slave` **`set rr-max 0`** `set ip-master 172.16.78.171` `next`

Bug ID	Description

```
    edit "slave2"
        set status disable
        set domain "test.edu"
        set type slave
        set rr-max 40000
        set ip-master 172.16.78.171
    next
end
```

Changes in default behavior

Bug ID	Description
598320	In a scenario where there are duplicate entries of `config icap server` with a duplicate combination of `ip-addresss`, `ip-version`, and `port`, the duplicate `config icap server` entries must be removed and replaced in the source data configuration (`config icap profile`). This step needs to be performed before upgrading in case of configuration loss.

Changes in default values

Bug ID	Description
548906	Change default extension information setting in `wtp-profile` from `disable` to `enable`. `config wireless-controller wtp-profile` `  edit <FAP-Profile>` `  **set ext-info-enable enable <== changed**` `  next` `end`
585889	Change default platform type setting in `wtp-profile` from `220B` to `221E`. `config wireless-controller wtp-profile` `  edit <New profile>` `  config platform` `  **set type 221E <== changed**` `  end` `  next` `end`
588382	Single 5G mode is the default setting for tri-radio AP models (FAP-U431F/U433F).
606533	Increase timeout from 10 s to 20 s when activating FortiGate Cloud from the web UI.

Changes in table size

Bug ID	Description
599271	Except for desktop models, all other platforms' table size of VIP real servers are increased as follows: • 1U platforms increased from 8 to 16 • 2U platforms increased from 32 to 64 • High-end platforms increased from 32 to 256
609785	Update number of supported FortiSwitch models per FortiGate platform.

New features or enhancements

Bug ID	Description
239809	Remove sticky clients by maintaining good SNR clients in BSS. Low SNR-based clients shall be deauthenticated and not allowed in BSS until SNR improves for these.
437116	For DFS-approved countries, add 160 MHz channel bonding support for FortiAP U421EV, U422EV, and U423EV models `config wireless-controller wtp-profile` `edit [ FAPU421EV-default | FAPU422EV-default | FAPU423EV-default ]` `config radio-2` `set band 802.11ac` `set channel-bonding` **`160MHz`** `end` `next` `end`
456803	Add virtual switch feature for FG-140E and FG-140E-POE.
457153	Support SSL VPN sign on using certificate and remote (LDAP or RADIUS) username/password authentication.
520828	Support VMWare tag filters in ESXi SDN connectors. Support obtaining and filtering of addresses by distributed port group names when a VM is attached to a distributed virtual switch.
529340	Decouple the memory size limit from the private VM license.
529445	In `wids-profile`, add the new `ap-scan-threshold` setting, which is the minimum signal level of rogue APs detected and required by the managed FortiAP devices. Only the rogue APs with a signal level higher than the threshold will be reported to the FortiGate WiFi Controller. `config wireless-controller wids-profile` `edit <WIDS-profile-name>` `set ap-scan enable` **`set ap-scan-threshold "-80"`** `next` `end` The range of `ap-scan-threshold`, in dBm, is -95 to -20 (default = -90).
532168	Support proxy traffic after TCP three-way handshake from client to original server for a specific port. CLI changes: • Add `proxy-after-tcp-handshake` option in protocol option and SSL-SSH profile.
553382	REST API to support transaction operation.
538760	Monitor API to check SLBC cluster checksum status. New API added - monitor/system/config-sync/status.
544704	Introduce 802.11ax support for FortiAP-U431F and FortiAP-U433F:

Bug ID	Description
	• Tri-radio support • Radio mode 11ax support • Dual 5G and single 5G mode support • HE (high efficiency)/160 MHz bandwidth/TWT support
550911	Merge *Dashboard*, *FortiView*, and *Monitor* pages.
553372	Under *Administrative Access*, *CAPWAP* and *FortiTelemetry* have been combined into one option labeled *Fabric Connection*. If either *CAPWAP* or *FortiTelemetry* were enabled on a particular interface, the new fabric option will be enabled after upgrading.
557614	FortiGate support for NSX-T v2.4: East/West traffic.
560138	External IP list (threat feed) object support added to security policy.
562394	Add support for EMS cloud. • Added CMDB attribute `fortinet-one-cloud-authentication` to FortiClient EMS table. • Added curl verbose diagnosis debugs to FortiClient NAC daemon for debug images. • Added `fortiems-cloud` option to type attribute in `user.fsso` table.
568528	Add IPv4 source guard to the switch controller. Added CLI command to push `ip-source-guard` static entries to FortiSwitch. • This feature enables source guard entries to be set for physical switches as well as trunk ports. • The source guard IP needs to be unique for every source guard entry across all ports. • The binding entry is a second level table (`switch_id` being the base) with `port_name` as the parent key. Deleted events work at a switch level, but the with second level tables, there is a need to store grandparent context as well. An opaque data field has been created in the queue node and the corresponding `flcfg_add_event_queue` and `flcfg_delete_sw_event_queue` have been modified accordingly. • Any calls to the `flcfg_add_event_queue` have been modified. • There are two kinds of events that will be generated with this command: `FLCFG_MSW_CMF_SOURCE_GUARD_UPDATE` for port level info change and `FLCFG_MSW_CMF_SOURCE_GUARD_ENTRY_UPDATE` for binding entry level info change.
569708	Support FSSO for dynamic addresses and support ClearPass endpoint connector (via FortiManager). CLI changes: • Add command to show FSSO dynamic address from authd daemon: `diagnose debug authd fsso show-address` • Make `diagnose firewall dynamic` commands to accept one optional parameter as address name: `diagnose firewall dynamic list` `diagnose firewall dynamic address` • Add FSSO subtype for firewall address: `config firewall address`

Bug ID	Description
	`` edit <name> set sub-type fsso next end ``` GUI changes: • Address dialog page • New subtype field to select between *FSSO* and *Fabric Connector* • New FSSO group field to select address group • Address list page • Tooltip for new FSSO dynamic address supports resolved address • *Detail* column shows the address groups for the address
570207	Support SAML method in firewall and SSL VPN authentications. CLI changes: • Add new CLI setting for SAML user: ``` config user saml edit * set ? cert Certificate to sign SAML messages. *entity-id SP entity ID. *single-sign-on-url SP single sign-on URL. single-logout-url SP single logout URL. *idp-entity-id IDP entity ID. *idp-single-sign-on-url IDP single sign-on URL. idp-single-logout-url IDP single logout url. *idp-cert IDP Certificate name. user-name User name in assertion statement. group-name Group name in assertion statement. next end ```
571639	Policy route changes: • Added *Hit Count* and *Last Used* columns for *Routing Monitor* > *Policy*, *Policy Route List*, and *SD-WAN Rules* pages. SD-WAN interfaces: • *SD-WAN* in navigation bar renamed *SD-WAN Interfaces*. • *SD-WAN Interfaces* list converted to a full page list with pie charts at the top. • Added *Sessions*, *Upload*, *Download* (bandwidth), *Bytes Sent*, and *Bytes Received* columns to the table. • The *Edit* dialog is no longer a slide in so it is consistent with other full page lists. SD-WAN rules: • Added a checkmark next to interface that is currently selected by SD-WAN. • Checkmark has *Member is selected* tooltip. A reason (*has best measured performances*/*meets most SLAs*) is further stated for *Best Performance* (priority) and *SLA* (SLA/load-balance) strategies.

Bug ID	Description
	• If multiple members are selected at the same time, GUI only marks the highest ranked member, unless mode is load-balance. • Added health check/SLA statistics tables for SD-WAN member omni select tooltip. • In the *Edit* dialog, the *Strategies* field changed to cards to allow a brief description of each strategy. • Added gutter to the *Edit* dialog. The gutter contains *Last used* and *Hit count* of the rule. • The gutter also contains a table showing statistics of currently selected members for SLA. • Added support for multiple members being selected in manual mode. Performance SLA: • Added support for IPv4 DNS protocol. • Added support for using system DNS. GUI will display the system DNS server in this case. • Support set members 0, which means all SD-WAN members participate in a health check.
571642	SD-WAN rule correlation improvement.
573176	Support destination MAC addresses in the sniffer traffic log.
573568	For FortiGate Azure HA, change public IP and routing table entries allocated in different resource groups. In an Azure HA scenario, EIP and route tables failover are specified in the SDN connector configuration. A new attribute, `resource-group`, was added, which allows a user to specifying the resource group that an EIP or route table is from. This new attribute can be empty so upgrade code is not required. If the `resource-group` of an EIP or route table is not provided, it is assumed the resource comes from the same resource group setting in the SDN connector (if there is no setting, it assumes the same resource group as the FortiGate itself by getting it from the instance metadata). CLI changes: • Add `resource-group` attribute.
573993	Add UTM log for FortiAnalyzer cloud-based subscription. CLI changes: • Default FortiAnalyzer Cloud filters set to enable `config log fortianalyzer-cloud filter` Most options within `config log fortianalyzer-cloud filter` defaulted to `disable` and could not be changed. Now, they default to `enable` and can be changed. License-based restrictions still apply, but the configuration can be used to refine the logs being sent to FortiAnalyzer Cloud. The exception is the `dlp-archive` option, which is still set to `disable` and cannot be changed.
575770	Increase IPS custom signature length to 4096.
576381	Automatically disable NPU offloading if the session interface has `shaping-profile` enabled.
577000	FortiGate debugger Chrome extension support. The extension improves the quality of GUI bug reports. The extension communicates with FortiOS and allows users to perform a capture. The capture includes (but is not limited to) the following: • Screen recording

Bug ID	Description
	• Device metadata • Client (browser) metadata • HTTP network logs • JavaScript console logs • Various daemon logs • Client memory and CPU usage • Device memory and CPU usage
577730	Authentication support for upstream/chained proxy in transparent mode.
578099	FortiAP profile support for FortiAP-231E NPI model. CLI changes: • Added `wtp-profile` support for FAP-231E NPI platform. • Multimode: single 5G and dual 5G same as U43xF with minor differences: • Single 5G • Radio 1 operates at 2.4 GHz • Radio 2 operates at 5 GHz • Radio 3 set to monitor mode • Dual 5G • Radio 1 operates at 5 GHz and uses the higher spectrum of channels (>= 64) • Radio 2: operates at 5 GHz and uses the lower spectrum of channels (< 64) • Radio 3: can be set to AP mode • New `wtp-profile` platform property `ddscan`. • FortiGate will configure DFS channels on FAP-231E with region code E, I, V, Y, and D. • Default mode for 3-radio AP models set to single 5G . GUI changes: • Added GUI support for FAP-231E platform: • New GUI option, *Dedicated scan*, which is counterpart of `ddscan` platform property. • When dedicated scan is enabled: • Monitor mode becomes exclusive to radio 3 • No AP mode for radio 3, even in dual 5G • No WIDS profile setting for radio 1 and 2 API changes: • /api/v2/monitor/wifi/ap_platforms • Radio property changed from object to array to accommodate for multimode platforms. First element is single 5G, and second is dual 5G platform radio configuration. For non-multimode platforms, array is of length 1.
578643	The feature extends the quarantine function on the FortiSwitch by allowing a device to be quarantined but remain with the VLAN where it was detected. The option to quarantine devices to a VLAN remains available.
578643	GUI changes in OCVPN to map user workflow habit.

Bug ID	Description
579484	Limit OCVPN spoke to only join existing overlay.
579899	Monitoring DHCP Pool via SNMP query and trap. • Added SNMP query OIDs (1.3.6.1.4.1.12356.101.23) for the following DHCP servers: • OID: 1.3.6.1.4.1.12356.101.23.1.1 • FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgDhcp.fgDhcpInfo.fgDhcpServerNumber • OID: 1.3.6.1.4.1.12356.101.23.2.1.1.2 • FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgDhcp.fgDhcpTables.fgDhcpTable.fgDhcpEntry.fgDhcpLeaseUsage • Added one SNMP trap (1301) for 3 DHCP events (DHCP server runs out of IP pool, IP address is already in use, or DHCP client interface received NAK). • In CLI, added `dhcp` option to `events` setting in SNMP configuration.
580048	NetFlow using HA reserved management interface.
580889	DPDK support on FortiOS VM platform.
581409	Allow administrators the ability to modify some configuration options of automatically generated VLANs by the switch controller. These changes are applied at the time of VLAN creation.
581412	Add automated detection and recommendations to configuration and conditions observed in the switch controller and FortiSwitch network. Administrators may accept the recommendations and have them automatically applied.
581742	Provide an integrated FortiGate network access control (NAC) function to the FortiAP and FortiSwitch networks by using a shared set of NAC policies. The NAC policy can be applied based on data from the user device list.
582241	Add antiphishing feature. The initial implementation adds functionality into WAD by parsing incoming HTTP requests, looking for known credentials, and if there is a match, performing the configured action.
582691	Extend SSL and certificate options in `ssl-ssh-profile`. `config firewall ssl-ssh-profile` `  edit "custom-deep-inspection"` `  set comment "Customizable deep inspection profile."` `  config ssl` `  set inspect-all disable` `  end` `  config https` `  set ports 443` `  set status deep-inspection` `  set proxy-after-tcp-handshake disable` `  set client-certificate bypass` **`  set unsupported-ssl-cipher allow  <==added`** **`  set unsupported-ssl-negotiation allow  <==added`**

Bug ID	Description
	set expired-server-cert block <==added **set revoked-server-cert block <==added** set untrusted-server-cert allow **set cert-validation-timeout allow <==added** **set cert-validation-failure block <==added** set sni-server-cert-check enable end next end
589374	Add client DHCP options. config system interface edit wan1 set mode dhcp .... config client-options edit 1 set code 60 set type {hex | string | ip | fqdn} set value|ip "xxxxxx" next end next end
591567	Support for additional SHA2 algorithms with SNMPv3.
593148	Update interface-related pages to use AngularJS and muTable. Interfaces list: • Radio buttons in the top-right corner let users switch between grouping by type, role, and sort lists alphabetically have been removed. There is a dropdown instead with the following options: • Group by type • Group by zone • Group by status, • Group by role • No grouping • Zones do not support parent-child relationships anymore. • The *DHCP Server* column has been divided into two separate columns, *DHCP Clients* and *DHCP Ranges*. • CSF support has been added. When switching to a downstream device, both the list and the faceplate should update. • For VDOMs, administrators can only view complete information about interfaces for the VDOM they are in. This applies even to administrators who have access to more than one VDOM. • On devices that support VLAN switching, the *VLAN Switch Mode* toggle has been removed

Bug ID	Description
	from the list page. It now shows up under *System> Settings*. • Faceplates do not auto-refresh on page load anymore. For auto-refresh, users need to enable the muTable refresh feature from the button in the bottom-right corner. Interfaces dialog: • Under *Administrative Access*, *CAPWAP* and *FortiTelemetry* have been combined into one option labeled *Fabric Connection*. • The secondary IP address toggle has been moved from the *Miscellaneous* section to the *Address* section. • A gutter has been added that displays the device hostname, the interface it belongs to, and relevant help links. CLI changes: • Consolidate `fortitelemetry` and `capwap` into `fabric` for `allowaccess` in `system.interface`.
593216	In order to more accurately detect Internet of Things (IoT), a new FortiGuard service provides a large database of device IoT identification. Devices detected on the local FortiGate and via FortiAP and FortiSwitch networks can be queried with the FortiGuard IoT device database to provide enhanced identification.
593262	Add prompt in CLI when creating a new VDOM.
596870	Add kernel support for the IEEE 802.1ad (QinQ) feature. In the past, 802.1Q specification allowed a single VLAN header to be inserted into an Ethernet frame. This new feature allows one more VLAN tag to be inserted into a single frame.
599826	Replace FSSO with REST API for EMS connector.
599925	Add option to enable/disable DFS zero wait functionality on FAP-U platforms.
601214	Support ADVPN peer-to-peer shortcuts through NAT. This solution provides hole punching support for RFC 4787 compliant NATs that use endpoint independent mapping. For a given source IP/port, the NAT mapping observed by the hub does not change when communicating with other endpoints, such as spoke-to-spoke shortcuts.
603216	Allow SD-WAN monitor to work on ADVPN shortcut. With this enhancement, SD-WAN can monitor link quality of the shortcut VPN between spoke-to-spoke. The SD-WAN service rules among spokes can accurately rely on SLA performance to determine which link to use. CLI changes: • Add a configurable probe count as number of most recent probes to calculate latency and jitter. • This new option is under `config system virtual-wan-link` > `config health-check` > `edit` a `health-check`.
605339	Add encryption option for FGSP.
607855	New subscription service for IoT device identification.

Bug ID	Description
612176	Support diffserv code setting for SD-WAN health hheck probe packet. When SD-WAN health check packet is sent out, the differentiated services code point (DSCP) can be set with the `set diffservcode` command: `config system virtual-wan-link` `config health-check` `edit h1` `....` **`set diffservcode <6-bits binary, range 000000-111111>`** `next` `end` `next` `end`

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- MAC-address-based policies – A new address type is introduced (MAC address range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.4.0 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.4.0 build 1992
- FortiClient EMS 6.4.0 build 1393
- FortiClient 6.4.0 build 1440
- FortiAP 5.6.5 and later
- FortiSwitch 3.6.11 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.0. When Security Fabric is enabled in FortiOS 6.4.0, all FortiGate devices must be running FortiOS 6.4.0.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.0 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.0 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)

- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.0 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.4.0 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.4.0, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.0.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.

- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.4.0. The *FortiView* page has been removed and merged in the *Top* standalone dashboards in the GUI by default.

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

Product integration and support

The following table lists FortiOS 6.4.0 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 72 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 27. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 27. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 27 and Fortinet Security Fabric upgrade on page 27. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0289 and later (needed for FSSO agent support OU in group filters) • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2008 R2 64-bit • Windows Server 2008 Core • Novell eDirectory 8.8
FortiExtender	• 3.2.1
AV Engine	• 6.00144
IPS Engine	• 6.00016
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 74 Google Chrome version 80
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 74 Google Chrome version 80
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Ubuntu 16.04 / 18.04	Mozilla Firefox version 54
OS X Catalina 10.15.2	Apple Safari version 13 Mozilla Firefox version 74 Google Chrome version 80
iOS	Apple Safari

Operating System	Web Browser
	Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 6.4.0. For inquires about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
557998	Quarantined CDR files cannot be downloaded. Encountered 404 error when clicking *Archived File*.
563250	Shared memory does not empty out properly under /tmp.
575177	Advanced threat protection statistics widget clean file count is incorrect.
590092	Cannot clear `scanunit vdom-stats` to reset the statistics on ATP widget.
594696	Sample file eicar.exe cannot pass through SMTPS, POP3S, or IMAPS with deep inspection and flow enabled on IPv6 policy.

Data Leak Prevention

Bug ID	Description
522472	DLP logs have a wrong reference link to archived file.
540317	DLP cannot detect attached zip files when receiving emails via MAPI over HTTP.
546964	DLP sensors and DLP options in firewall policy and profile groups are removed.
563447	Cannot download DLP archived file from GUI for HTTPS, FTPS, SMTP and SMTPS.
571171	Excessive false positives for credit card DLP profiles.
574722	DLP blocks Gmail with deep inspection.
586689	Downloading a file with an FTP client in EPSV mode will hang.
591178	WAD fails to determine the correct file name when downloading a file from Nextcloud.
591676	Enable file filter password protected blocked for 7Z, RAR, PDF, MSOffice, and MSOfficeX.

DNS Filter

Bug ID	Description
561297	DNS filtering does not perform well on the zone transfer when a large DNS zone's AXFR response consists of one or more messages.
563441	7K DNS filter breaking DNS zone transfer.
574980	DNS translation is not working when request is checked against the local FortiGate.
578267	DNS request to a second DNS server with same Transaction ID is discarded when DNS Filter is enabled on a policy.
581778	Cannot re-order DNS domain filter list.
582374	License shows expiry date of `0000-00-00`.
583449	DNS filter explicit block all (wildcard FQDN) not working in 6.2 firmware.
586526	Unable to change DNS filter profile category action after upgrading from 6.0.5 to 6.2.0.

Endpoint Control

Bug ID	Description
599826	Replace FSSO with REST API for EMS connector.

Explicit Proxy

Bug ID	Description
504011	FortiGate does not generate traffic logs for SOCKS proxy.
540091	Cannot access explicit FTP proxy via VIP.
571034	Using disclaimer causes incorrect redirection.
576205	App traffic cannot be blocked in a proxy policy with certificate inspection while it works in a firewall policy.
577372	WAD has signal 11 crash at `wad_ssl_cert_get_auth_status`.
578098	Unwanted traffic log generated for firewall policy with web filter profile as `MonitorAll`.
585310	Block page is not displayed for a URL in the frames of an allowed web page.
588211	WAD cannot learn policy if multiple policies use the same FQDN address.

Bug ID	Description
589065	FSSO-based NTLM sessions from explicit proxy do not respect timeout duration and type.
589166	EPSV does not work when using an FTP proxy.
589811	`urfilter` process does not started when adding a category as `dstaddr` in a proxy policy with the deny action.
590942	AV does not forward reply when GET for FTP over HTTP is used.
590959	FortiGate returns 500 internal error instead of `521 Not logged in - Secure authentication required`.
594580	FTP traffic over HTTP explicit proxy does not generate traffic logs once receiving error message.
594598	Enabling proxy policies (+400) increases memory by 30% and up to 80% total.
603707	The specified port configurations of `https-incoming-port` for `config web-proxy explicit` disappeared after rebooting.
605209	LDAP ignores `source-ip` with web proxy Kerberos authentication.
610298	Compare and sync the VSD change in V5.6 to WAD VS.

Firewall

Bug ID	Description
508015	Editing a policy in the GUI changes the FSSO setting to disable.
558996	FortiGate sends type-3 code-1 IP unreachable for VIP.
560011	Fabric device object does not work in NGFW policy.
570507	Application control causing NAT hairpin traffic to be dropped. **Workaround**: Create a new firewall policy from scratch and the default application control can be applied again.
574012	Session created by RPC session helper does not honor `delay-tcp-npu-session`.
577752	Policy with a VIP with a destination interface of a zone is dropping packets.
584451	NGFW default block page partially loads.
585073	Adding too many address objects to a local-in policy causes all blocking to fail.
585122	Should not be allowed to rename VIP or address with the same name as an existing VIP group or address group object.
590039	Samsung OEM internet browser cannot connect to FortiGate VS/VIP.
593103	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, ICMP unreachable message references the mapped address, not the external.

Bug ID	Description
595044	Get new CLI signal 11 crash log when performing `execute internet-service refresh`.
595364	Some NetFlows have an `active-flow-timeout` when the session does not have any packets and the session cache in NetFlow expires and clears.
596744	Firewall policy hit count is incorrect.
597110	When creating a firewall address with the `associated-interface` setting, CMD gets stuck if there is a large nested address group.
598000	When SCTP is in closing state and there is traffic passing through to keep it from timing out, even when an INIT is received, the traffic still passes through the old session.
598559	ISDB matches all objects and chooses the best one based on their weight values and the firewall policy.
599253	GUI traffic shaper *Bandwidth Utilization* should use KBps units.
600051	Cannot establish the connection to the real servers using VIP server load-balancing after upgrading to FortiOS 6.2.2.
600644	IPS engine did not resolve nested address groups when parsing the address group table for NGFW security policies.
601331	Virtual load-balance VIP and intermittent HTTP health check failures.
603263	Increase the maximum limit for the optional parameters in SCTP INIT packet. After the fix, the maximum limit is 10 instead of 4 parameters.
604886	Session stuck in proto_state=61 only when flow-based AV is enabled in the policy.
610557	FortiGate VIP object offers weak elliptic curves since VS implementation in WAD for FortiOS 6.0 and above.
611840	Firewall policy search with decimal in the name fails in GUI.
615073	FTP session helper does not work when there is reflected (auxiliary) session.

FortiView

Bug ID	Description
527540	Cannot click the *Quarantine Host* option on a registered device.
537819	FortiView *All Sessions* page tooltip for geography IP shows as *undefined*.
582341	On *Policies* page, consolidated policies are without names and tooltips; tooltips not working for security policies.

GUI

Bug ID	Description
282160	GUI does not show byte information for aggregate and VLAN interfaces.
303651	Should hide *Override internal DNS* option if `vdom-dns` is set to `disable`.
354464	*AntiVirus* profile in GUI should not override quarantine archive value.
438298	When VDOM is enabled, the interface faceplate should only show data for interfaces managed by the admin.
445074	The MMS profiles pages have been removed from the FortiOS Carrier GUI. **Workaround**: You can configure MMS profiles from the CLI using the `config firewall mms-profile` command.
451306	Add a tooltip for IPS *Rate Based Signatures*.
460698	There is no uptime information in the *HA Status* widget for the slave unit's GUI.
467495	A wrong warning message appears that the source interface has no members after enabling an inserted proxy policy.
478472	Options 150, 15, and 51 for the DHCP server should not be shown after removing them and having no related configuration in the backend.
480731	Interface filter gets incorrect result (EMAC VLAN, VLAN ID, etc.) when entries are collapsed.
482437	SD-WAN member number is not correct in *Interfaces* page.
486230	GUI on FG-3800D with 5.6.3 is very slow for configurations with numerous policies.
493527	Compliance events GUI page does not load when redirected from the advanced compliance page.
493704	While accessing the FortiGate page, PC browser memory usage keeps spiking and finally PC hangs.
498892	GUI shows wrong relationship between VLAN and physical interface after adding them to a zone.
502962	Get *Fail to retrieve info* for default VDOM link on *Network* > *Interfaces* page.
504829	GUI should not log out if there is a 401 error on the downstream device.
505066	Not possible to select value for DN field in LDAP GUI browser.
510685	*Hardware Switch* row is shown indicating a number of interfaces but without any interfaces below.
514027	Cannot disable CORS setting on GUI.
514632	Inconsistent `Refcnt` value in GUI when using ports in HA `session-sync-dev`.
525535	*OK* button greyed out when editing an interface that has DHCP option 224 in the list with *FortiClient-On-Net Status* enabled.
526254	Interface page keeps loading when VDOM admin have `netgrp` permission.
529094	*Anti-Spam Black White List Entry* in GUI permits action *Mark as Reject* in GUI when it should not.

Bug ID	Description
531376	Get *Internal Server Error* when editing an aggregate link that has a name with a space in it.
534853	Suggest GUI Interfaces list includes SIT tunnels.
536718	Cannot change MAC address setting when configuring a reserved DHCP client.
536843	LACP aggregate interface flaps when adding/removing a member interface (first position in member list).
537307	*Failed to retrieve info* message appears for `ha-mgmt-interface` in *Network* > *Interfaces*.
538125	Hovering mouse over FortiExtender virtual interface shows incorrect information.
540098	GUI does not display the status for VLAN and loopback in the *Network* > *Interfaces* > *Status* column.
542544	In *Log & Report*, filtering for blank values (*None*) always shows no results.
543487	*Collected Email Monitor* page cannot list the wireless client if connected from `captive-portal+email-collection`.
543637	Not able to filter the policy by multiple ID.
544442	Virtual IPs page should not show port range dialog box when the protocol is ICMP.
550911	Merge *Dashboard*, *FortiView*, and *Monitor* pages.
552038	Routing monitor network filter does not filter subnets after upgrading.
552623	Policy list page should not show inline editing icon in column field when logged in as a read-only user.
552811	Scripts pushed from FortiCloud do not show up in *System* > *Advanced Settings* when FortiCloud remote access is used.
553290	The tooltip for VLAN interfaces displays as *Failed to retrieve info*.
555121	Context menu of AP group has unsupported actions enabled after change view on Managed FortiAPs page.
555687	Network mask of a VPN interface is changed to 255.255.255.255 without an actual configuration change.
559799	Webhook automation host header incorrect.
559866	When sending CSF proxied request, segfault happens (httpsd crashes) if FortiExplorer accesses root FortiGate via the management tunnel.
560206	Change/remove FortiCloud standalone reference.
563053	Warning message for third-party transceivers were removed for 6.2.1 to prevent excessive RMA or support tickets. 6.2.2 re-added the warning for third-party transceivers.
564201	After OSPF change via GUI, password for virtual-link will completely disappear and must be re-entered.
565109	*Add Selected* button does not appear under *Application Control* slide-in when VDOM is enabled.

Bug ID	Description
565309	Application group improvements.
565748	New interface pair consolidated policy added via CLI is not displayed on GUI policy page.
566414	*Application Name* field shows `vuln_id` for custom signature, not its application name in logs.
566666	AP comments do not appear on the columns for *Managed AP* page.
567369	Cannot save DHCP *Relay* configuration when the *Relay* IP address list is separated by a comma.
567452	IPS sensor not configurable in GUI with Firefox.
568176	GUI response is very slow when accessing *Route Monitor* page in GUI.
569080	SD-WAN rule GUI page doesn't show red exclamation mark for DST-negate enabled, like firewall policy.
571909	*SSL VPN Settings* page shows undefined error.
573070	Interface widget not loading fully (keeps spinning) when a VDOM "prof_admin" is used.
573456	FortiGate without disk email alert settings page should remove *Disk usage exceeds* option.
573579	Editing policies inline can result in previously selected policies being changed.
573596	GUI shifts central management type to *FortiManager* after clicking *Apply* to enable *FortiManager Cloud*.
573869	Log search index files are never deleted when the log disk is out of space.
574101	Empty firmware version in managed FortiSwitch from FortiGate GUI.
575756	Port Link speed option is missing on the FortiGate GUI after upgrading the managed FortiSwitch to 6.2.1.
579259	*Firewall User Monitor* shows "Failed to retrieve info" and no entries if session-based proxy authentication is used.
579711	Cannot run *Security Rating* (Fabric device error).
580168	Connected routes in the routing monitor are showing up with *1969/12/31 18:59:59* for *Up Since* times.
582658	Email filter page keeps loading and cannot create a new profile when the VDOM admin only has `emailfilter` permission.
582716	Filtering service availability check always fails once anycast is enabled and override server is set.
583049	Internal server error while trying to create a new interface.
583760	After adding few web rating overrides via GUI to an already existing long list of URIs, *Web Rating Overrides* page does not load and keeps spinning.
584304	*IpSec Monitor* window *Bring Up* function does not work.
584314	NGFW mode should have a link to show all applications in the list.
584419	Issue with application and filter overrides.

Bug ID	Description
584426	*Add Selected* button does not show up under *FSSO Fabric Connector* with custom admin profile.
584560	GUI does not have the option to disable the interface when creating a VLAN interface.
584939	VPN event logs shows incorrectly when adding two action filters and if the filter action filter contains "-".
584949	When the link status is up, the aggregate interface status icon is incorrectly displayed in red.
585055	High CPU utilization by httpsd daemon if there are too many API connections
585924	Wrong traffic shaper bandwidth unit on 32-bit platform GUI pages.
586604	No matching IPS signatures are found when *Severity* or *Target* filter is applied.
586749	Enable/disable *Disarm and Reconstruction* in the GUI only affects the SMTP protocol in AV profiles.
587091	When logged in as administrator with web filter read/write only privilege, the *Web Rating Overrides* GUI page cannot load.
587673	On *Proxy Policy* page, the default view method (*Interface Pair View*) is not clickable.
588028	If the *Endpoint Control* feature is disabled, the exempt options for captive portal are not shown in the GUI.
588222	*WAN Opt. Monitor* displays *Total Savings* as negative integers during file transfers.
588665	Option to reset statistics from *Monitor* > *WAN Opt. Monitor* in GUI does not clear the counters.
589085	Web filter profile warning message when logged in with read/write admin on VDOM environment.
592244	VIPs dialog page should be able to create VIP with the same extip/extport but different source IP address.
593175	FortiGate with no anti-spam license is showing incorrect information under *FortiGuard* > *Filtering Services Availability*.
593433	DHCP offset option 2 has to be removed before changing the address range for the DHCP server in the GUI.
593624	GUI behavior is different with local user using super admin profile and TACACS user using super admin profile.
593899	Upgrading from build 0932 to build 1010 displays *Malware Hash Threat Feed is not found or enabled* error.
594162	Interface hierarchy is not respected in the GUI when a LAG interface belongs to SD-WAN and its VLANs belong to a zone.
594565	Wrong *Sub-Category* appears in the *Edit Web Rating Override* page.
598247	One-minute memory; *CPU* and *Sessions* widgets stopped updating after system entered and exited conserve mode.
598725	Login page shows random characters when system language is not English.

Bug ID	Description
599284	Pyfcgid crashed with `signal 11 (Segmentation fault) received`.
599401	FortiGuard quota category details displays *No matching entries found* for local category.
599612	GUI should allow user to create redundant IPsec tunnel over different interface to the same remote gateway.
601653	When deleting an AV profile in the GUI, there is no confirmation message prompt.
602397	FortiSwitch port page is noticeably slow for large topology.
602637	*Block intra-zone traffic* toggle button function is inverted in FortiOS 6.2.3.
602692	*Security Rating* result for SSL VPN certificate fails when using a 384-bit elliptic curve certificate.
603583	Data source is missing in child table entries in a complex type property.
605493	Admin cannot log in to FortiGate GUI.
605677	System goes into conserve mode when editing ISDB entries through GUI.
606074	*Interfaces* is missing in the GUI in sections for *IPv4 Policy* and *SSL-VPN Settings* after upgrading from 6.2.2 to 6.2.3.
606295	Cannot activate or log out of FortiGate Cloud from widget.
606394	DPD setting in GUI cannot be reflected correctly when *Dialup User* and *On Demand* are set by the IPsec wizard.
607972	FortiGate enters conserve mode when accessing Amazon AWS ISDB object.
607982	*Edit DNS Filter Profile* page cannot be displayed if botnet domain is enabled.
609064	*Revoke Token* in GUI reports URL not found on server.
610191	Multiple behavior changes to both CLI and GUI: • Added default automation rules (after factory reset). All are disabled by default, except for the FEXP push notification. • Added new incoming webhook trigger for automation. • Removed *Email Alert Settings* page. • Added new API for `POST /api/v2/monitor/system/automation-stitch/webhook/<trigger mkey>`.
610573	When saving configuration under global interface, explicit proxy settings are removed.
611436	FortiGate displays a hacked web page after selecting an IPS log.
601345	No warning is shown in GUI when FortiGuard filtering protocol/port setting is not saved.
617364	GUI does not list AliCoud SDN address filter.

HA

Bug ID	Description
530215	Application `hasync` returns "*** signal 11 (Segmentation fault) received ***".
540632	In HA, `management-ip` that is set on a hardware switch interface does not respond to ping after executing reboot.
543602	Unnecessary syncing process started during upgrade when it takes longer.
568553	Read-only admin account can failover a HA.
569629	HA A-A local FQDN not resolving on slave unit.
574564	In an HA configuration with HA uninterruptible upgrade enabled, some signature database files may fail to synchronize upon upgrading from 5.6.9 and earlier to 5.6.10.
575020	HA failing `config sync` on VM01 with error (slave and master have different hdisk status) when master is pre-configured.
575715	Unable to sync the local gateway in FGSP.
576638	HA cluster GUI change does not send logs to the slave immediately.
577115	Master unit console keeps showing message `[ha_auth_set_logon_msg:228] buffer overflow`.
578475	FortiGate HA reports not synced if firewall policy of master and slave does not contain the same VIP.
581906	HA slave sending out GARP packets in 16-20 seconds after HA monitored interface failed.
584551	`hatalk` keeps exchanging heartbeat packet incorrectly with FortiManager.
585348	`default-gateway` injected by `dynamic-gateway` on PPP interface deleted by other interface down.
585675	`exe backup disk alllogs ftp` command causes FortiGate to enter conserve mode.
586004	Moving VDOM via GUI between virtual clusters causes cluster to go out of sync and VDOM state work/standby does not change.
586835	HA slave unable to get checksum from master. HA sync in `Z` state.
588291	SIP HA message could overwhelm HA slave box and drive the slave box to conserve mode.
588908	FG-3400E `hasync` reports the network is unreachable.
590632	Heartbeat device (interface) up messages not triggered.
590931	Multiple PPPoE connections on a single interface does not sync PPPoE dynamic assigned IP and cannot start re-negotiation.
596837	Deleting tunnel on master via API call will not delete it from the slave unit.
596575	HA active-active master attempts to steer HTTP and SMTP sessions to slave unit over NPU-VLINK interfaces.

Bug ID	Description
598937	Local user creation causes HA to be out of sync for several minutes.
601550	Application `hasync` crashes several times.
602266	The configuration of the SD-WAN interface gateway IP should not sync.
602406	In a FortiGate HA cluster, performance SLA (SD-WAN) information does not sync with the slave unit.
613714	HA failover takes over one minute when monitored aggregate interface goes down on master.

ICAP

Bug ID	Description
598320	New constraint added in `config icap server` entries in FortiOS ICAP client feature.

Intrusion Prevention

Bug ID	Description
540718	Signal 14 alarm crashes were observed on DFA rebuild.
561623	IPS engine 5.009 crashes when updated new FFDB has different size from the old one.
579018	IPS engine 5.030 signal 14 alarm clock crash at `nturbo_on_event`.
586608	The CPU consumption of ipsengine gets high with customer configuration file.
590087	When IPS pcap is enabled, traffic is intermittently disrupted after disk I/O reaches IOPS limit.
608501	IPS forwards attacks that are previously identified as dropped.

IPsec VPN

Bug ID	Description
449212	New dialup IPsec tunnel in policy mode/mode-cfg overwrites previously established tunnel.
557812	IPsec does not support the new `interface-subnet` type in its `phase2-interface` and `ipv4-split-include` settings for dialup VPN.
574115	PKI certificates with OU and/or DC as subject fail for PKI user filters.

Bug ID	Description
575238	Redirected traffic on the same interface (ingress and egress interface are the same) is dropped.
575477	IKED memory leak.
577502	OCVPN cannot register - status "Undefined".
582251	IKEv2 with EAP peer ID authentication validation does not work.
582876	ADVPN connections from the hub disconnects one-by-one and IKE gets stuck.
584982	The customer is unable to log in to VPN with RADIUS intermittently.
589096	In IPsec after HA failover, performance regression and IKESAs is lost.
589141	Dialup IPsec tunnel DPD discrepancy.
594962	IPsec VPN IKEv2 interoperability issue when the FortiGate uses a group as P2 selectors with a non-FortiGate in a remote peer gateway.
595810	Unable to reach network resources via L2TP over IPsec with WAN PPPoE connection.
596429	Traffic unable to pass through for certain phase 2 selectors when there is double SA.
597246	When disabling and re-enabling OCVPN after HA failover, cannot establish IPsec tunnel.
597748	L2TP/IPsec VPN disconnects frequently.
597845	IPsec VPN over IPv6 ISAKMP SA negotiation failure when setting is IPv4 DHCP mode.
599471	IKEv2 responder can delete static selectors when local narrowing occurs.
602240	IKEv2 EAP-TLS handshake detected retransmit of client, but FortiGate does not retransmit its response.
604334	L2TP disconnection when transferring large files.
604923	IKE memory leak when IKEv2 certificate subject alternative name/peer ID matching occurs.
606129	`iked` crashes when proposal is AES-GCM.
607212	IKEv2 DPD is not triggered if network overlay network ID was mismatched when first configured.
609033	After two HA failovers, one VPN interface member of SD-WAN cannot forward packets.
610390	IKEv2 EAP certificate authentication failings after upgrading from to 6.2.1 to 6.2.3.
611148	L2TP/IPsec does not send framed IP address in RADIUS accounting updates.
617419	FortiGate does not assign correct system DNS value to the client connected to dialup VPN.

Log & Report

Bug ID	Description
568795	Specific traffic type is not logged on FortiAnalyzer/memory.

Bug ID	Description
576024	Set sniffer policy to only log `logtraffic=utm` but many traffic log stats are still generated in disk or FortiAnalyzer.
578057	Action field in traffic log cannot record security policy action—it shows the consolidated policy action.
580887	No traffic log after reducing miglogd child to 1.
583499	Improve local log search logic from aggressive to passive mode to save resources and CPU.
586038	FortiOS 6.0.6 reports too long VPN tunnel durations in local report.
586854	FortiGate sends change notice for global REST APIs once a minute.
590598	Log viewer application control cannot show any logs (page is stuck loading).
590852	Log filter can return empty result when there are too many logs, but the filter result is small.
591152	IPS logs set `srcintf(role)/dstinf(role)` reversely at the time of IPS signature reverse pattern.
591523	When refreshing logs in GUI, some `log_se` processes are running extremely long and consuming CPU.
593363	Total sum of `vdom log-disk-quota` can be set to surpass total HD logging space.
593557	Logs to syslog server configured with FQDN addresses fail when the DNS entry gets updated for the FQDN address.
593907	Miglogd still uses the daylight savings time after daylight savings ends.
594053	Proxy policy forward traffic log should have "timeout" action for no-reply or timeout case.
599860	When `logtraffic` is set to `all`, existing sessions cannot change the egress interfaces when the routing table is updated with a new outgoing interface.
602459	GUI shows *401 Unauthorized* error when downloading forward traffic logs with the time stamp as the filter criterion.
605174	Incorrect `sentdelta/rcvddelta` in traffic log statistics for RTSP sessions.
606533	User observes `FGT internal error` while trying to log in from the web UI.
608565	FortiGate sends incorrect long session logs to FortiGate Cloud.

Proxy

Bug ID	Description
519861	FortiGate does not bypass the forward server if upstream proxy is down and `server-down-option` is set to `pass`.
525328	External resource does not support no content length.
549660	WAD crash with signal 11.
550056	When SNI is exempt in an SSL profile, and the SNI does not match the CN, the FortiGate closes the session and does not perform deep inspection.
551119	Certificate blacklist not working correctly in proxy mode.
560893	When strict SNI check is enabled, FortiGate with certificate inspection cannot block session if SNI does not match CN.
561552	WAD crashed with signal 6 (MAPI/RPC).
566859	In WAD conserve mode 5.6.8, `max_blocks` value is high on some workers.
567942	FortiGate cannot block blacklist certificate against TLS 1.3 if the blacklist certificate server address is exempt.
572489	SSL handshake sometimes fail due to FortiGate replying back `FIN` to client.
573028	WAD crash causing traffic interruption.
573721	For FortiGate with client certificate inspect mode, traffic will trigger WAD crash.
573917	Certain web pages time out.
574171	Fail to connect https://drive.google.com by TLS 1.3.
574730	Wildcard URL filter stops working after upgrade.
576852	WAD process crashes in `internet_svc_entry_cmp`.
579225	FTP proxy traffic is blocked for FSSO guest users.
579400	High CPU with `authd` process caused by WAD paring multiple line content-encoding error and IPC broken between `wad` and `authd`.
580592	Policy in proxy-based mode with AV and WAF profile denies access to Nginx with enabled gzip compression.
580770	SSL decryption breaks App store and Google Play store traffic even though both sites are exempted in the decryption profile.
580943	FortiGate blacklist certificate info is not shown in replace message on certificate inspect case in TLS 1.3.
581865	In Proxy inspection with Application control and certificate inspection, TLS error for certain web pages, in EDGE browser only.
582475	WAD is crashing with signal 6 in `wad_fmem_free` when processing SMB2/CIFS.

Bug ID	Description
582714	WAD might leak memory during SSL session ticket resumption.
583736	WAD application crashing in 6.2.1.
584719	WAD reads `ftp over-limit multi-line` response incorrectly.
586909	When CIFS profile is loaded, using MacOS to access Windows Share causes WAD to crash.
587214	WAD crash for `wad_ssl_port_on_ocsp_notify`.
587987	In case of TLS 1.3 with certificate inspection and a certificate with an empty CN name, WAD workers would locate a random size for CN name and then cause unexpected high memory usage in WAD workers.
589065	FSSO-based NTLM sessions from explicit proxy do not respect timeout duration and type.
592153	Potential memory leak that will be triggered by certificate inspection CIC connection in WAD.
593365	WAD crash due to user learned from proxy not purged from the kernel when user is deleted from proxy or zone with empty interface member.
594725	WAD memory leak detected on `cert_hash in wad_ssl_cert`.
594829	FTP connection is not working with AV profile in proxy inspection mode when FTP user name contains an "@".
596012	Receive SSL fatal alert with source IP 0.0.0.0.
608387	WAD virtual server with `http-multiplex` enabled causes crash after server is detached because the http_server object is detached from http_session.

REST API

Bug ID	Description
450175	Cannot modify `ge` and `le` attributes for `router prefix-list` table without plugin flag.
553382	REST API to support transaction operation.
587470	REST API to support revision flag.
599516	When managing FortiGate via FortiGate Cloud, sometimes user only gets read-only access.
601613	CMDB plugin should be called when saving data through CMDB REST API.

Routing

Bug ID	Description
371453	OSPF translated type 5 LSA not flushed according to RFC-3101.
524229	SD-WAN `health-check keep` records useless logs under some circumstances.
537354	BFD/BGP dropping when `outbandwidth` is set on interface.
570686	FortiOS 6.2.1 introduces asymmetric return path on the hub in SD-WAN after the link change due to SLA on the spoke.
571714	DHCPv6 relay shows *no route to host* when there are multiple paths to reach it.
576930	Time stamps missing in routing debugs.
578623	Gradual memory increase with full BGP table.
581488	BGP confederation router sending incorrect AS to neighbor group routers.
582078	ISDB ID is changed after restoring the configuration under the situation where the FortiGate has a previous ISDB version.
584095	SD-WAN option of `set gateway enable`/`set default enable` override available on connected routes.
584394	VRRP on LAG cannot forward packet after `vrrp-virtual-mac` is enabled.
584477	In transparent mode with asymmetric routing, packet in the reply direction does not use asymmetric route.
585027	There is no indication in `proute` if the SD-WAN service is default or not.
585325	IPv6 route cannot be inactive after `link-monitor` is down when `link-monitor` are set with `ipv4` and `ipv6`.
587198	After failover/recovery of link, E2 route with non-zero forward address recurses to itself as a next hope.
587700	Routing monitor policy view cannot show source and destination data for SD-WAN route and wildcard destination.
587970	SD-WAN rules `route-tag` still used in service rule but not in `diagnose sys virtual-wan-link route-tag-list`.
589620	Link monitor with tunnel as `srcintf` cannot recover after remote server down/up.
592599	FortiGate sends malformed OSPFv3 LSAReq/LSAck packets on interfaces with MTU = 9k.
593375	OSPF NSSA with multiple ASBR losing valid external OSPF routes in upstream neighbors as different ASBRs are power cycled.
593864	Routing table is not always updated when BGP gets an update with changed next hop.
593951	Improve algorithm to distribute ECMP traffic for source IP-based/destination IP-based.
594685	Unable to create the IPsec VPN directly in *Network* > *SD-WAN*.

Bug ID	Description
595937	PPPoE interface bandwidth is mistakenly calculated as 0 in SD-WAN.
597733	IPv6 ECMP routes cannot be synchronized correctly to HA slave unit.
598665	BGP route is in routing table but not in FIB (kernel routing table).
599667	OSPF over ADVPN flapping after shortcut tunnel established.
599884	Traffic not following SD-WAN rules when one of the interfaces is VLAN.
600332	SD-WAN GUI page bandwidth shows 0 issues when there is traffic running.
600598	SSH packets marked as CS0.
600830	SD-WAN health check reports have packet loss if response time is longer than the check interval.
600995	Policy routes with large address groups containing FQDNs no longer work after upgrading to 6.2.2.
602223	SD-WAN route is not added in routing table when the SD-WAN interface members are IPv4 over IPv6 IPsec.
602679	Prevent BGP daemon crashing when peer breaks TCP connection.
603063	Locally originated traffic on non-default VRF may follow route on VRF 0 when there are routes with the same prefix on both VRFs.
611539	Editing/adding any address object that is referenced in policy is generating false positive SD-WAN alert messages.
611708	Make SNMP get BGP peer state timely once BGP neighbor enters or exits established state.

Security Fabric

Bug ID	Description
575495	FGCP dynamic objects are not populated in the slave unit.
586024	Automation stitch cannot execute shutdown command when FortiGate enters kernel conserve mode.
586587	Security Fabric widget keeps loading when FortiSwitches are in a loop, or the FortiSwitch is in MCLAG mode.
587758	Invalid CIDR format shows as valid by the Security Fabric threat feed.
588262	IP address *Threat Feed* fabric connector not working.
589503	*Threat Feeds* show the URL is invalid if there is a special character in the URL.
591015	ACI SDN connector dynamic address cannot be resolved.
592344	CSF automation configuration cannot be synced to downstream from root.
599474	FortiGate SDN connector not seeing all available tag name-value pairs.

Bug ID	Description
604670	Time zone of scheduled automation stitches will always be taken as GMT-08:00 regardless of the system's `timezone` configuration.
606714	`auto-script` returns `failed to get SCSI info from /dev/mmcblk0` memory error.

SSL VPN

Bug ID	Description
476377	SSL VPN FortiClient login with FAC user FTM two-factor fail because it times out too fast.
478957	SSL VPN web portal login history is not displayed if logs are stored in FortiAnalyzer.
491733	When SSL VPN receives multiple HTTPS post requests under web filter, `read_request_data_f` loops even when client is stopped, which causes the SSL VPN process to use 99% of CPU.
525342	In some special cases, SSL VPN main state machine reads function pointer is empty that will cause SSL VPN daemon crash.
537341	SSL bookmark is not loading SAP portal information.
549994	SSL VPN web mode logon page should not show *Skip* button for remote user with *Force password change on next logon*.
556657	Internal website not working through SSL VPN web mode.
557806	Cannot fully load a website through SSL VPN bookmark.
558685	Two-factor authentication with FortiToken easily bypassed when using LDAP authentication.
560438	`interface` subnet object not available in SSL VPN `split-tunneling-routing-address`.
561585	SSL VPN does not correctly show Windows Admin center application.
563022	SSL VPN LDAP group object matching only matches the first policy; is not consistent with normal firewall policy.
564871	SSL VPN users create multiple connections.
569711	Error for proxy SSH database through SSL VPN.
570171	When accessing ACT application through SSL VPN web mode, the embedded calendar request gets wrong response and redirects to login page.
570445	CMAT application through SSL VPN.
571721	Local portal `adzh-srop-nidm02.intern.cube.ch` needs more than 10 min. to load via SSL VPN bookmark.
572653	Unable to access Qlik Sense URL via SSL VPN web mode.
573787	SSL VPN web mode not displaying custom web application's JavaScript parts.
573853	TX packet drops on `ssl.root` interface.

Bug ID	Description
574551	Subpages on internal websites are not working via SSL VPN web mode (Tunnel mode is OK).
574724	SSL VPN conserve mode on FWF-30E when FortiGate unit enters memory less than 25%.
575259	SSL VPN connection is being dropped intermittently.
576013	The SSL VPN web mode webserver link is not rewritten correctly after login.
576288	FSSO groups set in rule with SSL VPN interface.
577522	SSL VPN daemon crashes when logging in several times with RADIUS user that is related to a framed IP address.
578581	SSL web mode VPN portal freezing when opening some websites using JavaScript.
578908	Fails to load bookmark site over SSL VPN portal.
580182	The EOASIS website is not displayed properly using SSL VPN web mode.
580377	Unable to access https://outlook.office365.com as bookmark in SSL VPN web mode.
580384	SSL VPN web mode not redirecting URL as expected after successful login.
581863	Accessing http://nlyte.ote.gr/nlyte/ configured with bookmark name 'NLYTE' not getting authentication page.
582115	Third-party (Ultimo) web app does not load over SSL VPN web portal.
582161	Internal web application is not accessible through web SSL VPN.
582265	RDP sessions are terminated (disconnect) unexpectedly.
583339	Support HSTS `include SubDomains` and `preload` option under SSL VPN settings.
584780	When the SSL VPN portal theme is set to red, the style is lost in the SSL VPN portal.
585754	A VPN SSL bookmark failed to load the Proxmox GUI interface.
586032	Unable to download report from an internal server via SSL VPN web mode connection.
586035	The policy "`script-src 'self'`" will block the SSL VPN proxy URL.
587075	SAML login is not stable for SSL VPN, it requires restarting `sslvpnd` to enable the function.
587300	In web mode, third-party webpage stuck on loading animation; JavaScript error in console.
587732	The SSL VPN web mode SSH widget is not connecting to the SSH server.
588066	SSO for HTTPS fails when using "\" (backslash) with the domain\username format.
588119	There is no OS support for the latest macOS Catalina version (10.15) when using SSL VPN tunnel mode.
588587	Different portals of SIPLAN COMPESA do not show properly in web mode.
588720	SSL VPN web portal bookmarks cannot resolve `hostname`.
589015	SSO does not correctly URL-encode POST-ed credentials.

Bug ID	Description
590643	`href` rewrite has some issues with the customer's JS file.
590663	Most charts and diagrams on the website could not be shown in SSL VPN web mode when using a special tool.
592318	After `sslvpn proxy`, some Kurim JS files run with an error.
592935	sslvpnd crashed on FortiGate.
593082	SSL VPN bookmark does not load Google Maps on internal server.
593367	SSL VPN bookmark does not load after clicking from the portal.
593621	Website not fully loading through web portal bookmark; loads correctly with iPad user agent.
593641	Cannot access HTTPS bookmark, get a blank page.
593850	SSL VPN logs out after some users click through the remote application.
594160	Screen shot feature is not working though SSL VPN portal.
594247	Cannot access https://cdn.i-ready.com through SSL VPN web portal.
595505	FortiGate does not send client IP address as a framed IP address to RADIUS server in RADIUS accounting request message.
595627	Cannot access some specific sites through SSL VPN web mode.
595920	SSL VPN web mode goes to 99% on a specific bookmark.
596273	sslvpnd worker process crashes, causing a zombie tunnel session.
596296	SSL VPN fails 90% when connecting with FortiClient.
596352	SAML user name is not correctly recorded in logs when logging in to SSL VPN portal via SSO entry, and history cannot be shown.
596412	Not possible to download PDF file after connecting to portal through SSL VPN bookmark.
596441	FortiOS does not correctly re-write the Exchange OWA logoff URL when accessed via SSL VPN bookmark.
596757	SSL VPN connection stuck at 95% or 98%.
596843	Internal website not working in SSL VPN web mode.
596846	Unable to deauthenticate FSSO user in GUI, but it works in CLI.
597282	The latest FortiOS GUI does not render when accessing it by the SSL VPN portal.
597336	Webpage does not load properly through SSL VPN web mode (fails to show CAPTCHA).
597566	Add SSL VPN SSO user logged in from SAML response.
597634	In SSL VPN web mode, internal web services not working and tunnel mode is working fine.
597658	Internal custom web application page running on Apache Tomcat is not displaying in SSL VPN web mode.

Bug ID	Description
598659	SSL VPN daemon crash.
598660	Internal website is not accessible from SSL VPN as the URL is being modified.
599394	SSL VPN web portal bookmarks are not full loading for Vivendi SelfService application.
599668	In SSL VPN web mode, page keeps loading after user authenticates into internal application.
599671	In SSL VPN web mode, cannot display complete content on page, and cannot paste or type in the comments section.
599777	Problem with ratm.avanzasa.com portal accessed via SSL VPN web mode.
599960	RADIUS user and local token push cannot log in to SSL VPN portal/tunnel when the password needs to be changed.
600029	Sending RADIUS accounting interim update messages with SSL VPN client framed IP are delayed.
600098	Unable to access internal web URL via web mode in Safari browser.
600103	sslvpnd crashes when trying to query a DNS host name without a period (.).
601084	Site in .NET framework 4.6 or 4.7 not loading in SSL VPN web mode.
601867	SSL VPN web mode cannot open DFS share subdirectories, gives invalid HTTP request message.
602392	Cannot access remote site using SSL VPN web mode after upgrading to FOS 6.2.2.
602645	SSL VPN synology NAS web bookmark log in page does not work after upgrading to 6.2.3.
603518	Internal website not working in SSL VPN web mode; cannot load ESS/MSS page.
603524	Download progress is not shown for the FTP files of the SSL portal.
603779	Chinese characters are garbled when downloading from SMB/CIFS in SSL VPN web mode.
603817	Internal website is not shown properly in SSL VPN web mode.
603957	SSL VPN LDAP authentication does not work in multiple user group configurations after upgrading the firewall to 6.0.7.
604882	Internal SAP website not working in SSL VPN web mode.
604910	Remedy application website is not accessible from SSL VPN as the URL is being modified.
605110	Mobile token is not required when LDAP user and LDAP group are set in SSL VPN policy together.
605699	Internal HRIS website dropdown list box not loading in SSL VPN web mode.
606094	SSL VPN web mode is not working; SSL VPN portal cannot be accessed.
606271	Double redirection through SSL web mode not working.
607687	RDP connection via SSL VPN web portal does not work with UserPrincipalName (UPN) and NLA security.
608195	AngularJS web application cannot load via SSL VPN web mode.
610247	SSL VPN access topinfo.gdfxpz -- AnyGlass website problem with SSL VPN web bookmark.

Bug ID	Description
610366	Webpage keep loading using through SSL VPN and bookmark.
610579	Videos from live cameras via SSL VPN web mode not working.
613641	SSL VPN web mode custom FortiClient download URL with %s causing sslvpnd to crash.
614528	Customer unable to load website through SSL VPN web mode.

Switch Controller

Bug ID	Description
517663	On a managed FortiSwitch already running the latest GA image, *Upgrade Available* is shown.
527695	On a network running FortiSwitch prior to 6.0.0, a `syn-error` occurs. The network will still function normally. **Workaround**: Users with 6.0.x should upgrade to remove the `sync-error` or disable `vlan-optimization`. On a network with `switch-controller.global.vlan-all-mode all` configured, the setting will revert to the default value of `defined`. Users who wish to maintain the `vlan-all-mode all` behavior may restore it after upgrading.
557280	Need to add FortiSwitch port information on Security Fabric and device inventory the same as before 6.0.4.
581370	FortiSwitch managed by FortiGate not updating the RADIUS settings and user group in the FortiSwitch.
586299	Adding factory-reset device to HA fails with `switch-controller.qos` settings in root.
592111	FortiSwitch shows offline CAPWAP response packet getting dropped/failed after upgrading from 6.2.2.
595671	`set key-outbound` and `set key-inbound` parameters are missing for GRE tunnel in `config system gre-tunnel`.
601547	Unable to push user group configuration from FortiGate to FortiSwitch, and `user.group` configuration is deleted.
607707	Unable to push configuration changes from FortiGate to FortiSwitch.
608231	LLDP policy did not download completely to the managed FortiSwitch 108Es.
613323	FortiSwitch trunk configuration sync issue after FortiGate failover.

System

Bug ID	Description
398024	Some error padding formats of SHA-256 SSL encrypted packets can stop the output function of command queue in CP8.
444611	Firewall policy is deleted after a hard power cycle and subsequent file system check and reboot.
470875	OID seems to be COUNTER32 instead of GAUGE32.
484749	TCP traffic with `tcp_ecn` tag cannot go through `ipip ipv6 tunnel` with NP6 offload enabled.
511790	Router info does not update after plugging out/plugging in USB modem.
519209	`diagnose` command on VDOM disclose other VDOM information.
527459	SDN address filter unable to handle space character.
527599	Internal prioritization of OSPF/BGP/BFD packets in conjunction with HPE feature to ensure these routing packets are handled in time. It affects all NP6 platforms.
528052	FortiGuard filtering services show as unavailable for read-only admin.
544570	Master unit does not send SNMP trap for all SNMP servers if the cable is plugged out from the interface configured as LAG.
547712	HPE does not protect against DDoS attacks like flood on IKE and BGP destination ports.
550206	Memory (SKB) which is no longer needed is not released in NP6 and NP6lite drivers (FG-100E, FG-140E, FG-3600D, FG-3800D).
556408	Aggregate link does not work for LACP mode active for FG-60E internal ports but works for wan1 and wan2 combination.
567487	CPU goes to 100% when modifying members of an `addrgrp` object.
570227	FortiGate is not selecting an NTP server that has a clock time in the majority clique of other NTP servers.
570575	PoE ports no longer deliver power.
570759	RX/TX counters for VLAN interfaces based on LACP interface are 0.
570834	STP (spanning tree) flapping.
572003	There was a hardware defect in an earlier revision of SSD used for FG-61E. When powering off then powering on in a very short time, the SSD may jump into ROM mode and cannot recover until a power circle.
572763	softirq causing high CPU when session increase in an acceptable way.
573090	Making a change to a policy through inline editing is very slow with large table sizes.
573177	GUI cannot save edits made on replacement messages in a VDOM. When using CLI, user gets logged out while editing.
573238	Session TTL expiry timer is not reset for VLAN traffic when offloading is enabled.

Bug ID	Description
573973	ASIC offloading sessions sticking to interfaces after SD-WAN SLA interface selection.
574086	Kernel panic occurs after upgrading from 6.2.0 to 6.2.1.
574110	When adding admin down interface as a member of aggregate interface, it shows up and process the traffic.
574327	FortiGate CSR traffic to SCEP server generated from the root VDOM instead of the VDOM createf for the CSR.
574716	ospfNbrState OID takes too long to update.
574991	FortiGate can't extract the user principal name `UPN` from user certificate when certificate contains UPN and additional names.
576337	SNMP polling stopped when FortiManager API script executed onto FortiGate.
576389	Cannot see the IP in `diag ip address` list if the secondary IP is deleted, set as the primary IP, and `secondary-IP` is disabled.
577047	FortiGate takes a long time to reboot when it has many firewall addresses used in many policies.
577302	Virtual WAN Link process (vwl) memory usage keeps increasing after upgrading to 6.2.1.
577423	FG-80D and FG-92D kernel error in CLI during FortiGate boot up.
578259	FG-3980E VLANs over LAG interface show no TX/RX statistics.
578269	Mismatch between number of lists with CPU usage OID and number of CPU threads.
578531	`forticldd` deamon resolved `mgrctrl1.fortinet.com` to wrong IP address.
578608	High CPU usage due to dnsproxy process as high at 99%.
578746	FortiGate does not accept FortiManager created country code and causes address install fails.
579524	DHCP lease is not stable and `dhcpd` process crashes.
580038	Problems with cmdbsvr while handling a large number of FSSO address groups and security policies.
580185	`authd4` crashes when deleting a VDOM or rebooting the FortiGate.
580883	DNS servers acquired via PPPoE in non-management VDOMs are used for DHCP DNS server option 6.
581496	FG-201E stops sending out packets and NP6lite is stuck.
581528	SSH/RDP sessions are terminated unexpectedly.
581998	Session clash event log found on FG-6500F when passing a lot of the same source IP ICMP traffic over load-balance VIP.
582520	Enabling offloading drops fragmented packets.
582547	`fgfmsd` crash makes connection to FortiManager go down.
583199	`fgfmsd` crashed with signal 11 when some code accesses a VDOM that has been deleted, but does not check the return value from CMDB query.

Bug ID	Description
583602	Script to purge and re-create a local-in-policy ran against the remote FortiGate directly (in the CLI) is causing auto-update issues.
586301	GUI cannot show default Fortinet logo for replacement messages.
586551	When an SD-WAN member is disabled or VWL is disabled, `snmpwalk` shows "No Such Object available on this agent at this OID" message.
587498	FortiGate sends ICMP type 3 code 3 (port unreachable) for UDP 500 and UDP 520 against vulnerability scan.
587521	VIP server load-balancing persistence HTTP cookie not refreshed after the timer.
587540	NetFlow traffic records sent with wrong interface index 0 (`inputint = 0` and `outputint = 0`)
587995	Packet loss happened in FTP traffic for some cases.
588035	Kernel crashes when sniffing packets on interfaces that are related to EMAC VLAN.
588202	FortiGate returns invalid configuration during FortiManager retrieving configuration.
589027	EMAC VLAN drops traffic when asymmetric roue enabled on internet VDOM.
589079	QSFP interface goes down when the `get system interface transceiver` command is interrupted.
589234	Local system DNS setting instead of DNS setting acquired from upstream DHCP server was assigned to client under management VDOM.
589517	Dedicated management CPU running on high CPU (soft IRQ).
589723	Wrong source IP is bound for `config system fortiguard`.
589978	`alertemail username` length cannot go beyond 35 characters.
590021	Enabling `auto-asic-offload` results in keeping `action=deny` in traffic log with an accept entry.
590295	OID for the IPsec VPN phase 2 selector only displays the first one on the list.
590423	FortiManager needs patch and minor number to update global database when FortiGate firmware upgrade does not trigger an auto-retrieve configuration.
591466	Cannot change the mask for an existing secondary IP on interfaces.
592148	Issue with TCP packets when traversing the virtual wire pair in transparent mode.
592570	VLAN switch does not work on FG-100E.
592787	FortiGate got rebooted automatically due to kernel crash.
592827	FortiGate is not sending DHCP request after receiving offer.
593426	Remove DST for Brazil.
593606	`diagnose hardware test suite all` fails due to FortiLink loopback test.
594018	Update daemon is locked to one resolved update server.

Bug ID	Description
594499	Communication over PPPoE fails after installing PPPoE configuration from FortiManager.
594596	Crash caused by JSON filter because a null check is not done.
594865	`diagnose internet-service match` does not return the IP value of the IP reputation database object.
595338	Unable to execute `ping6` when configuring `execute ping6-options tos`, except for `default`.
595467	Invalid multicast policy created after transparent VDOM restored.
596180	Constant DHCPD crashes.
596421	FG-3400E/FG-3600E link is up on 25G ports only when the FEC is disabled on the Ixia tester.
598527	ISDB may cause crashes after downgrading FortiGate firmware.
600032	SNMP does not provide routing table for non-management VDOM.
601454	For 32-bit system, there is no `bandwidth-unit` option in `traffic-shaper`, but the `guaranteed-bandwidth`/`maximum-bandwidth` help text still says `Units depend on the bandwidth-unit setting`.
601866	nTurbo set IRQ affinity as failed when platform has quite a few PCIe devices and many interrupts are requested during system bootup.
602523	DDNS `monitor-interface` uses the monitored interface if DDNS services other than FortiGuard DDNS are used.
602548	Some of the clients are not getting their IP through DHCP intermittently.
602643	Interfaces get removed from SD-WAN after rebooting when interface is defined in both SD-WAN and zone.
603551	DHCPv6 relay does not work on FG-2200E.
604550	Locally-originated DHCP relay traffic on non-default VRF may follow route on VRF 0.
604613	`sentbyte` of NTP on local traffic log shows as `0` bytes, even though NTP client receives the packet.
604699	Five FG-30Es and one FG-100D enter in conserve mode in a transparent mode deployment.
606597	When changing time zone on FG-101E, get *Failed to set SMC timezone* message.
607015	Too many DNS lookups with global NTP server as global NTP server often changes its IP.
607357	High CPU usage issue caused by high depth expectation sessions in the same hash table slot.
607452	Automatically logged out of CLI when trying to configure STP due to /bin/newcli crash.
608185	Number of resource records is limited to 16384 on DSN server.
608442	After a reboot of the PPPoE server, the FortiGate (PPPoE clients, 35 clients) keeps flapping (connection down and up) for a long time before connecting successfully.

Bug ID	Description
608648	FortiCarrier 3000D kernel panic when establishing GTP tunnel.
610470	A single IP existing in IP range format may cause some issues in other daemons.
610903	SMC NTP functions are enabled on some of the models that do not support the feature.
612113	xcvrd attaches shared memory multiple times causing huge memory consumption.
612302	FortiOS is not sending out IPv6 router advertisements from the link-local addresses added on the fly.
612351	Many `no session matched` logs while managing FortiGate.
613017	`ip6-extra-addr` does not perform router advertisement after reboot in HA.
613410	Host header has been added to the HTTP 1.0 request for CRL file.
616022	Long delay and cmdbsvr at 100% CPU consumption when modifying address objects and address groups via GUI or REST API.

Upgrade

Bug ID	Description
580450	Policies were removed after an upgrade in NGFW policy mode. Error message that *Maximum number of entries has been reached*.
586123	Service group lost default members when restoring a configuration file via VDOM.
586793	Address objects have reference to old firewall policy after upgrading from 6.0.6 > 6.2.x NGFW policies.

User & Authentication

Bug ID	Description
466651	The FortiToken Mobile push functionality on the FortiGate lacks the ability to map to a custom SSL certificate.
557947	Non-RSSO RADIUS server shows in FSSO GUI, which should only show RSSO RADIUS servers.
567831	Local FSSO poller regularly missing logon events.
573317	SSO admin with a user name over 35 characters cannot log in after the first login.
581519	Creating SCEP enrollment in context global no longer seems to work if VDOM is configured as the management VDOM.

Bug ID	Description
583745	Wrong categorization of OS from device detection.
586334	Brief connectivity loss on shared service when RDP session is logged in to from local device.
586394	Authentication list entry is not created/updated after changing the client PC with another user in FSSO polling mode.
587293	The session to the SQL database is closed as `timeout` when a new user logs in to terminal server.
587519	fnbamd takes high CPU usage and user not able to authenticate.
587666	Mobile token authentication does not work for SSL VPN on SOC3 platforms. Affected models include: FG-60E, FG-60E-POE, FG-61E, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-100E, FG-100EF, FG-101E, FG-140E, FWF-60E, FWF-61E.
591461	FortiGate does not send user IP to TACACS server during authentication.
592047	GUI RADIUS test fails with `vdom-dns` configuration.
592241	Gmail POP3 authentication fails with certificate error since version 6.0.5.
592253	RADIUS state attribute truncated in access request when using third-party MFA (ping ID).
593116	Client PC matching multiple authentication methods (firewall, FSSO, RSSO, WSSO) may not be matched to NGFW policies correctly.
593361	No source IP option available for OCSP certificate checking.
593949	Two-factor LDAP and token authentication silently fails for users with many memberships.
594863	UPN extraction does not work for particular PKI.
595583	Device identification of LLDP on an aggregate does not work.
596844	Admin GUI login makes the FortiGate unstable when there are lots of devices detected by device identification.
597118	URL redirection is not supported when making up a certificate chain list.
597496	Guest user log in expires after first log in and no longer works; user is not removed from the firewall authentication list after the set time.
603457	Guest user groups cannot be deleted.
605206	FortiClient server certificate in FSSO CA uses weak public key strength of 1024 bits and certificate expiring in May 2020.
605404	FortiGate does not respond to disclaimer page request when traffic hits a disclaimer-enabled policy with thousands of address objects.

VM

Bug ID	Description
524052	Application `cloudinitd` has signal 11 crash on FortiGate-VM64-GCP.
561909	Azure SDN connector tries querying invalid FQDN when using Azure Stack integrated systems.
571212	Only one CPU core in AWS is being used for traffic processing.
575346	`gui-wanopt` cache missing under system settings after upgrading a FortiGate VM with two disks.
575400	In Azure SDN, the firewall address filter cannot fetch the secondary public and private IP addresses of the NICs.
577653	vMotion tasks cause connections to be dropped as sessions related to vMotion VMs do not appear on the destination VMX.
577856	Add missing AWS HA failover error log and set firewall.vip/vip46/vip6/vip64 not syncing when cross zone HA is configured.
578727	FG-VM-OPC unable to failover the route properly during failover.
578966	OpenStack PCI pass through sub-interface VLAN cannot receive traffic.
579708	Should replace GUI option to register to FortiCare from AWS PAYG with link to portal for registration.
579948	New FGCP master is not updated in AWS route tables to reference the correct ENI.
580738	In the cluster setup, slave unit can have different fingerprint for the OCI SDN connector, which can cause unit to fail to connect to the OCI metatdata server properly.
580911	EIP assigned to the secondary IP address on the OCI does not fail over during HA failover.
582123	EIP does not failover if the master FortiGate is rebooted or stopped from the Alibaba Cloud console.
586954	FGCP cluster member reboots in infinite loop and `hatalk` daemon dumps the core with segmentation fault.
587757	FG-VM image unable to be deployed on AWS with additional HDD(st1) disk type.
588436	Azure SDN connector unable to connect to Azure Kubneretes integrated with AAD.
589445	VM deployed in ESX platform with VMXNET3 does not show the correct speed and duplex settings.
590140	FG-VM-LENC unable to validate new license.
590149	Azure FortiGate crashing frequently when MLX4 driver RX jumbo.
590253	VLAN not working on FortiGate in a Hyper-V deployment.
590555	Allow PAYG AWS VM to bootstrap the configuration first before acquiring FortiCare license.
590780	Azure FortiGate-VM (BYOL) unable to boot up when loading a lower vCPU license than the instance's vCPU.

Bug ID	Description
591563	Azure autoscale not syncing after upgrading to 6.2.2.
592000	In Alibaba Cloud, multiple VPC route entries fail to switch when HA fails over.
592611	HA not fully failing over when using OCI.
593797	FG-VM64-AWS not responding to ICMP6 request when destination IPv6 address is in the neighbor cache entry.
594248	Enabling or disabling SR-IOV under vNIC creates duplicate MAC addresses and extra interfaces on the FortiGate.
597003	Unable to bypass self-signed certificates on Chrome in macOS Catalina.
598419	Static routes are not in sync on FortiGate Azure.
599430	FG-VM-AZURE fails to bootup due to `rtnl_lock` deadlock.
600975	Race condition may prevent FG-VM-Azure from booting up because of deadlock when processing NETVSC offering and vPCI offering at the same time.
601357	FortiGate VM Azure in HA has unsuccessful failover.
601528	License validation failure log message missing when using FortiManager to validate a VM.
603365	HA slave member instance shuts down due to RAM difference after stopping/starting the cluster instances.
603599	VIP in autoscale on GCP not syncing to other nodes.
605103	E1000 network adapter will be deleted if there is a VMXNET3 network adapter.
605435	API call to associate elastic IP is triggered only when the unit becomes the master.
606439	License validation failure log message missing when using FortiManager to validate a VM.
609283	IP pools are synchronized in FortiGate Azure HA.
612611	Very hard to download image for FG-AWSONDEMAND from FDS.
614038	VMotion causing sessions to be disconnected as sessions are considered stateless.

VoIP

Bug ID	Description
570430	SIP ALG generates a VoIP session with wrong direction.
580588	SDP information fields are not being NATted in multipart media encapsulation traffic.
582271	Add support for Cisco IP Phone keepalive packet.
599117	`voipd` process crash.
601275	MGCP session helper does not NAT the MGCP body.

Web Filter

Bug ID	Description
551956	Proxy web filtering blocks innocent sites due to `urlsource="FortiSandBox Block"`.
560904	In NGFW mode, *Security Profiles* GUI is missing *Web Rating Overrides* page.
581523	Wrong web filter category when using flow-based inspection.
587120	Administrator logged in with web filter read/write privilege cannot create or edit web filter profiles in the GUI.
593203	Cannot enter a name for a web rating override and save—error message appears when entering the name.
606965	Unable to whitelist specific YouTube channel when all other YouTube channels or videos are blocked.

WiFi Controller

Bug ID	Description
520677	When editing a FortiAP profile on the FortiGate web UI, the previously selected SSID group(s) cannot be displayed.
540027	FortiWiFi working as client mode cannot see and connect to the hotspot SSID from iOS devices.
555659	When FortiAP is managed with cross VDOM links, the WiFi client cannot join to SSID when `auto-asic-offload` is enabled.
559370	`darrp-optimize-schedules` configurations move to the global settings instead of VDOM.
563630	Kernel panic observed on FWF-60E.
564318	Move `frequency-handoff`/`ap-handoff` from radio level to AP level.
566054	Errors pop up while creating or editing as SSID.
567011	WPA2-Enterprise SSID should support `acct-all-servers` setting in RADIUS to send accounting messages to all servers.
567933	FortiAP unable to connect to FortiGate via IPsec VPN tunnel with `dtls-policy clear-text`.
572350	FortiOS GUI cannot support FAP-U431F and FAP-U433F profiles. **Workaround**: Edit `wtp-profile` of FAP-U431F and FAP-U433F in the CLI.
577394	hostapd (wpad_ac) crashed while removing RADIUS accounting servers.
579908	Tunnel mode SSID packet loss seen from FAP-U24JEV and 800 connected APs.
580169	Captive portal (disclaimer) redirect not working for Android phones.

Bug ID	Description
580793	Auto-generated consolidated policy should skip saving in configuartion file/CMDB.
594170	FortiAPs not shown in the GUI.
595653	FortiGate in transparent mode cannot manage FortiAP devices successfully.
599690	Unable to perform COA with device MAC address for 802.1x wireless connection when `use-management-vdom` is enabled.
601012	When upgrading from 5.6.9 to 6.0.8, channels 120, 124, and 128 are no longer there for NZ country code.
608717	Packet loss over CAPWAP tunneled SSID.
615219	FortiGate cannot create WTP entry for FortiAP in transparent mode.
615615	Add support for VLAN probe on *Managed FortiAPs* summary details GUI page.

Known issues

The following issues have been identified in version 6.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
618718	`set certificate` configuration missing in `config endpoint-control fctems` after rebooting.

GUI

Bug ID	Description
622510	Page is stuck and there is a blank message field when doing policy lookup with non-IP protocol.

IPsec VPN

Bug ID	Description
622506	L2TP over IPsec tunnel established, but traffic cannot pass because wrong interface gets in route lookup.

SSL VPN

Bug ID	Description
616429	Local user assigned with FortiToken cannot log in to SSL VPN web/tunnel mode when password change is required.
616879	Traffic cannot pass through FortiGate for SSL VPN web mode if the user is a PKI peer.

Switch Controller

Bug ID	Description
607753	CAPWAP is not updated to be a Fabric connection after upgrading from 6.4.0 Beta1 build 1519 to build 1538.
621785	`user.nac-policy[].switch-scope` may contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, they need to remove this reference prior to deleting the `managed-switch`.
622812	VLANs on a FortiLink interface configured to use a hardware switch interface may fail to come up after upgrading or rebooting.

System

Bug ID	Description
587824	Member of virtual WAN link lost after upgrade if management interface is `set dedicated-to management` before.

User & Authentication

Bug ID	Description
606327	FTM push return traffic (mobile device to FortiGate) has TLS handshake failure; same device with 6.2.3 GA is OK.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.